MATHEMATICS

SUR LES THEOREMES FONDAMENTAUX DES GROUPES FORMELS COMMUTATIFS. I

PAR

MICHEL LAZARD

(Communicated by Prof. N. H. KUIPER at the meeting of December 16, 1972)

Les théorèmes fondamentaux en question sont d'abord ceux qui établissent une équivalence entre la catégorie des groupes formels commutatifs sur un anneau K et celle de certains modules topologiques sur un anneau, qui dépend fonctoriellement de K et peut être remplacé par un anneau plus petit quand certains nombres premiers sont inversibles dans K. Ensuite ces théorèmes établissent des propriétés relatives à la définition (par générateurs et relations) des modules topologiques précités.

Le présent travail doit son existence, entre autres, à Pierre Cartier, à qui sont dédiés les foncteurs Cart et Cart_S. On observera que la notion d'hyperalgèbre (ou bigèbre), présentée par certains comme fondamentale, n'apparaît même pas ici. Par contre, toute la théorie repose sur les opérateurs F_n de Cartier et sur le "théorème des fantômes", c'est-à-dire, en dimension finie, les propriétés et les relations mutuelles des bourgeons et des lois de groupes universels. Ce dernier théorème a été jugé par Manine "presque inapplicable" [1]).

N.B. Après la rédaction de la présente note, j'ai eu connaissance des travaux de M. Hazewinkel (Constructing formal groups I. Over $\mathbf{Z}_{(p)}$-algebras. Report 7119 + appendix of the Econometric Inst. Netherlands School of Economics, Rotterdam; Constructing formal groups II. Over $\mathbf{Z}$-algebra. Report 7201, ibid.) et de F. J. DITTERS (Groupes formels à un paramètre sur $\mathbf{Z}$ et $\mathbf{Z}_{(p)}$. C.R. Acad. Sci. Paris, 275 (1972) p. 251–254). On trouvera notamment chez le premier une formule explicite donnant le logarithme d'un groupe formel p-typique universel.

I. FONCTEURS DE CARTIER [2]) ET MODULES RÉDUITS

1. *Propriétés générales des foncteurs* Cart_S. Nous désignerons par S un ensemble de nombres premiers, et par la lettre grasse correspondante $\mathbf{S}$

[1]) Yu. I. MANIN, Théorie des groupes formels commutatifs sur des corps de caractéristique finie (en russe), Usp. Mat. Nauk 18 (1963) p. 3–90; traduction anglaise: Russian Mathematical Surveys, 18 (1963) p. 1–84. Cet article contient une bibliographie de 60 titres. On trouvera une autre bibliographie dans l'exposé de I. BARSOTTI, Sviluppi e applicazioni della teoria dei gruppi analitici commutativi, Atti dell' VIII Congresso dell' Unione Matematica Italiana, Trieste 1967.

[2]) P. Cartier: 1. Groupes formels associés aux anneaux de Witt généralisés (C.R. Acad. Sc. Paris, 265 (1967) p. 50–52); 2. Modules associés à un groupe formel commutatif. Courbes typiques (Ibid. p. 129–132).

l'ensemble des entiers ($\geqslant 1$) dont tous les facteurs premiers sont dans S. A chaque S correspond un foncteur, noté Cart_S, qui associe à tout anneau commutatif unitaire K un anneau topologique complet $\mathrm{Cart}_S(K)$, unitaire mais non commutatif en général [3]). L'anneau $\mathrm{Cart}_S(K)$ contient des éléments notés V_n^K, F_n^K où $n \in \mathbf{S}$, et $[c]$ où $c \in K$. Tout élément $x \in \mathrm{Cart}_S(K)$ s'écrit *univoquement* comme une somme infinie convergente:

$$x = \sum_{m,n \in \mathbf{S}} V_m^K [c_{m,n}] F_n^K, \tag{1.1}$$

où les $c_{m,n} \in K$ (dits coordonnées de x) doivent vérifier la seule condition
(1.2) *pour tout $m \in \mathbf{S}$, l'ensemble des n tels que $c_{m,n} \neq 0$ est fini.*

Si $f: K \to K'$ est un homomorphisme d'anneaux, l'image de x par l'homomorphisme associé $\mathrm{Cart}_S(f): \mathrm{Cart}_S(K) \to \mathrm{Cart}_S(K')$ est

$$\sum_{m,n \in \mathbf{S}} V_m^{K'} [f(c_{m,n})] F_n^{K'}. \tag{1.3}$$

Fixant S et K, nous écrirons V_m, F_n, E au lieu de V_m^K, F_n^K, $\mathrm{Cart}_S(K)$. Un élément $x \in E$ est nul si toutes ses coordonnées $c_{m,n}$ sont nulles; sinon son *ordre*, noté ord (x), est le plus petit m tel qu'existe un $c_{m,n} \neq 0$; nous posons ord $(0) = +\infty$. L'axiome

$$\operatorname{ord}(x \pm y) \geqslant \min(\operatorname{ord}(x), \operatorname{ord}(y)) \quad \text{pour tous } x, y \in E \tag{1.4}$$

est satisfait, et les sous-groupes additifs (en fait idéaux à droite) définis par les conditions ord $(x) \geqslant n$ ($n \in \mathbf{S}$) forment un système fondamental de voisinages de 0 dans E. Les relations suivantes sont vérifiées:

$$V_1 = F_1 = [1_K] = 1_E; \tag{1.5}$$

$$V_m V_n = V_{mn},\ F_m F_n = F_{mn},\ [a][b] = [ab], \text{ pour tous } m, n \in \mathbf{S},\ a, b \in K; \tag{1.6}$$

$$\text{si } m, n \in \mathbf{S} \text{ et } pgcd\ (m, n) = 1, \text{ alors } V_m F_n = F_n V_m; \tag{1.7}$$

$$\text{pour tout } n \in \mathbf{S},\ F_n V_n = n\ 1_E; \tag{1.8}$$

$$[c] V_n = V_n [c^n] \text{ et } F_n [c] = [c^n] F_n \text{ pour tous } n \in \mathbf{S} \text{ et } c \in K; \tag{1.9}$$

$$\operatorname{ord}([a] + [b] - [a+b]) > 1 \text{ pour tous } a, b \in K. \tag{1.10}$$

Les propriétés précédentes définissent complètement le foncteur Cart_S. En considérant l'opération naturelle à droite de E sur $gr_1(E)$, composante de degré 1 du gradué associé (qui s'identifie au K-module libre de base les F_n), on obtient la représentation matricielle $\varkappa$ de E, qui associe à $x = \sum V_m [c_{m,n}] F_n$ la matrice

$$\varkappa(x) = \sum_{m,n,i \in \mathbf{S}} m c^i_{m,n}\, \mathbf{e}_{mi,ni}, \tag{1.11}$$

où les $\mathbf{e}_{i,j}$ désignent les unités matricielles indexées par les entiers de S

[3]) Les exceptions sont les suivantes: 1°) $S = \emptyset$; alors $\mathrm{Cart}_S(K) = K$; 2°) $S = \{p\}$, $K = \mathbf{F}_p$; alors $\mathrm{Cart}_S(K)$ est une certaine extension commutative de l'anneau des entiers p-adiques; 3°) $K = \{0\}$; alors $\mathrm{Cart}_S(K) = \{0\}$.

$(\mathbf{e}_{i,j}\mathbf{e}_{k,l}=\delta_{j,k}\mathbf{e}_{i,l})$. Les coefficients $\varkappa(x)_{i,j}$ de $\varkappa(x)$ s'écrivent, en posant $r=pgcd\ (i,j)$:

$$\varkappa(x)_{i,j}=\textstyle\sum_{d|r}\ (di/r)\,c^{r/d}_{di/r,\,dj/r}. \tag{1.12}$$

Les éléments de la forme $\sum_{n\in \mathbf{S}} V_n[a_n]F_n$, représentés par des matrices diagonales, constituent un *sous-anneau commutatif* de $\mathrm{Cart}_S(K)$, qu'on peut identifier à l'anneau $W_S(K)$ des S-vecteurs de Witt, lui-même quotient de $W(K)$ (cf. Cartier 1). Pour définir sans confusion possible l'*opération à gauche* de $\mathrm{Cart}_S(K)$ sur $W_S(K)$, nous préférons noter un élément de $W_S(K)$ comme un vecteur $\xi=(a_i)_{i\in\mathbf{S}}$ à coordonnées dans K, et désigner par "op" l'isomorphisme qui associe à ξ l'opérateur

$$\mathrm{op}\ (\xi)=\textstyle\sum_{i\in\mathbf{S}}\ V_i[a_i]F_i\in \mathrm{Cart}_S(K).$$

Alors l'opération de $\mathrm{Cart}_S(K)$ sur $W_S(K)$ est définie par les formules suivantes:

$$\mathrm{op}\ ([c]\cdot\xi)=[c]\ \mathrm{op}\ (\xi)=\ \mathrm{op}\ (\xi)[c]; \tag{1.13}$$

$$\mathrm{op}\ (V_n\cdot\xi)=V_n\ \mathrm{op}\ (\xi)F_n; \tag{1.14}$$

$$\mathrm{op}\ (\xi)V_n=V_n\ \mathrm{op}\ (F_n\cdot\xi)\ \text{ et }\ F_n\ \mathrm{op}\ (\xi)=\ \mathrm{op}\ (F_n\cdot\xi)F_n. \tag{1.15}$$

Cette dernière relation montre que $\xi\mapsto F_n\cdot\xi$ est un endomorphisme de $W_S(K)$ et s'explicite ainsi pour $\xi=(a_i)_{i\in\mathbf{S}}$ et $n\in\mathbf{S}$:

$$\mathrm{op}\ (F_n\cdot\xi)=\textstyle\sum_{i\in\mathbf{S}}\,d\,V_{i/d}[a_i^{n/d}]F_{i/d},\ \text{ où }\ d=pgcd\ (i,n). \tag{1.16}$$

Les multiples entiers de l'unité se calculent dans $\mathrm{Cart}_S(K)$ comme dans $W_S(K)$, et un entier n est inversible dans $\mathrm{Cart}_S(K)$ s'il est inversible dans K.

Si $S'\subset S$, l'anneau $\mathrm{Cart}_{S'}(K)$ s'identifie à un quotient du sous-anneau fermé de $\mathrm{Cart}_S(K)$ engendré par les $[c]$ et les V_n, F_n, où $n\in\mathbf{S}'$.

2. *La décomposition* (*ou "typification"*). Nous considérons ici une *partition* $\{S',S''\}$ d'un ensemble S de nombres premiers et un anneau K où *tous les* $p\in S'$ *sont supposés inversibles*. Nous posons $E=\mathrm{Cart}_S(K)$. Nous avons alors dans E les idempotents permutables $(1-p^{-1}V_pF_p)$, où $p\in S'$; le produit de ces idempotents converge, et nous le désignons par π:

$$\pi=\textstyle\prod_{p\in\mathbf{S}'}\ (1-p^{-1}V_pF_p)=\sum_{n\in\mathbf{S}'}\ n^{-1}\mu(n)V_nF_n, \tag{2.1}$$

μ désignant la fonction de Möbius. Nous avons

$$\pi V_n=F_n\pi=0\ \text{ pour tout }\ n\in\mathbf{S}',\ n\neq 1. \tag{2.2}$$

(2.3) Si C (resp. M) est un E-module topologique à gauche (resp. à droite), alors πC (resp. $M\pi$) est l'intersection des noyaux des opérateurs F_p (resp. V_p) où $p\in S'$ dans C (resp. M), tandis que $(Id_C-\pi)C$ (resp. $M(Id_M-\pi)$) est l'adhérence de la somme des images des opérateurs V_p (resp. F_p) dans C (resp. M), pour $p\in S'$.

(2.4) *Le sous-anneau* $\pi E\pi$ (dont l'unité est π, distincte de celle de E si $S' \neq \emptyset$) *est canoniquement isomorphe à l'anneau* $E'' = \mathrm{Cart}_{S''}(K)$. L'isomorphisme associe à

$$x = \sum_{i,j \in S''} V_i[c_{i,j}]F_j \in E''$$

l'élément *de même ordre*

$$\sum_{n \in S',\, i,j \in S''} n^{-1}\mu(n) V_{ni}[c_{i,j}^n]F_{nj} \in \pi E\pi.$$

(2.5) Posons, pour tout $n \in \mathbf{S}'$, $\varrho_n = n^{-1} V_n \pi F_n$ (en particulier $\varrho_1 = \pi$). Alors les ϱ_n sont des *idempotents de E, deux à deux orthogonaux, d'ordres respectifs n et de somme* 1_E.

(2.6) Théorème. *L'anneau* $E = \mathrm{Cart}_S(K)$ *est canoniquement isomorphe à un anneau de matrices* $y = (y_{m,n})$ *à coefficients dans* $E'' = \mathrm{Cart}_{S''}(K)$ *indexés par les entiers* $m, n \in \mathbf{S}'$. *Les matrices sont astreintes à la seule condition que, pour tout* $m \in \mathbf{S}'$, ord $(y_{m,n})$ *tende vers l'infini avec* n.

En effet, on écrit $x \in E$ sous la forme $\sum_{m,n \in S'} x_{m,n}$, où $x_{m,n} = \varrho_m x \varrho_n$, on pose $z_{m,n} = m^{-1} F_m x_{m,n} V_n \in \pi E \pi$, puis on remplace chaque $z_{m,n}$ par l'élément correspondant $y_{m,n}$ de E'' (2.4). On retrouve x par les relations $x_{m,n} = n^{-1} V_m z_{m,n} F_n$. En particulier si $S' = S$, $S'' = \emptyset$, alors $E'' = K$ et la matrice associée à x est $N^{-1}\varkappa(x)N$, où $N = \sum_{n \in S} n\, \mathbf{e}_{n,n}$.

3. *Modules uniformes et modules réduits.* Nous appelons *E-module uniforme* un E-module à gauche topologique complet C possédant la propriété suivante:

(3.1) *les sommes infinies* $\sum_{j \in J} x_j \gamma_j$ (*où* $x_j \in E$, $\gamma_j \in C$) *convergent dans* C *sous la seule hypothèse que* ord $(x_j) \to +\infty$ (*suivant le filtre des complémentaires des parties finies de l'ensemble* J).

Nous notons E_V l'ensemble des éléments de E qui s'écrivent sans F, i.e. sous la forme $\sum_{n \in S} V_n[c_n]$, et nous disons que $(\gamma_i)_{i \in I}$ est une famille de *V-générateurs* (resp. une *V-base*) dans un E-module uniforme C si tout élément $\gamma \in C$ s'écrit (resp. s'écrit *univoquement*) sous la forme $\sum_{i \in I} x_i \gamma_i$ où $x_i \in E_V$ pour tout $i \in I$ (et ord $(x_i) \to \infty$ si I est infini). Nous appelons *E-module réduit* un E-module uniforme qui possède une V-base.

(3.2) Proposition. *Soient C un E-module réduit et, pour tout* $n \in \mathbf{S}$, C_n (*resp.* C_{n+}) *l'adhérence de la somme des sous-groupes additifs* $V_m \cdot C$ *pour* $m \geqslant n$ (*resp.* $m > n$); *posons* $gr_n(C) = C_n/C_{n+}$. *Alors chaque opérateur* V_m *induit un isomorphisme de* $gr_n(C)$ *sur* $gr_{mn}(C)$. *Le groupe* $gr_1(C)$ *a une structure naturelle de K-module libre, et les V-bases de C sont les familles d'éléments dont les images* modulo C_{1+} *sont les bases de* $gr_1(C)$ *sur* K.

La topologie définie par les C_n est plus fine que la topologie donnée de C (c'est la plus fine pour laquelle C reste un E-module uniforme).

(3.3) Sous les hypothèses de décomposition précisées en (2), la catégorie des E-modules uniformes (resp. des E-modules réduits) est *équivalente* à celle des E''-modules uniformes (resp. des E''-modules réduits): cela résulte de (2.5) et (2.6).

4. *Quotients de modules uniformes-libres.* Soit $x = \sum_{i,j \in S} V_i[c_{i,j}]F_j$ un élément non nul de $E = \mathrm{Cart}_S(K)$. Nous appelons *type* de x, et notons $tp(x)$, le couple (m, n) où $m = \mathrm{ord}\,(x)$ et n est *le plus grand* entier j tel que $c_{m,j} \neq 0$. Soit $\alpha \in \mathbf{R}$ la borne inférieure des i/j pour $c_{i,j} \neq 0$. La *hauteur* de x, notée $ht(x)$, est par définition α si la borne inférieure est atteinte; sinon (ce qui ne peut arriver que si $\mathrm{Card}\,(S) > 1$), nous écrivons $ht(x) = \alpha +$ (nombre "semi-réel" immédiatement supérieur à α). Nous posons $tp(0) = (\infty, 0)$ et $ht(0) = +\infty$. Nous ordonnons les types par la relation

$$(4.1) \qquad (m, n) > (m', n') \Leftrightarrow m > m' \text{ ou } (m = m' \text{ et } n < n'),$$

et nous convenons que "$tp(x) \geqslant (m, 0)$" signifie "$\mathrm{ord}\,(x) > m$". Le lemme suivant justifie la distinction entre α et $\alpha+$.

(4.2) Soient $x, y \in E$, $ht(x) = h > 0+$, $tp(y) = (m, n)$. Alors $tp(yx) \geqslant (m, p.e.(n/h))$, où "$p.e.(n/h)$" désigne la partie entière, définie comme le plus grand entier $\leqslant n/\alpha$ (resp. $< n/\alpha$) si $h = \alpha$ (resp. $h = \alpha+$).

Soient I un ensemble et L le E-module *uniforme-libre* admettant comme base topologique la famille $(\gamma_i)_{i \in I}$: chaque élément $\gamma \in L$ s'écrit univoquement

$$\gamma = \textstyle\sum_{i \in I} x_i \gamma_i,$$

avec $x_i \in E$ (et $\mathrm{ord}\,(x_i) \to \infty$ quand I est infini). Pour un tel γ nous posons

$$(4.3) \qquad \mathrm{ord}\,(\gamma) = \min_i \mathrm{ord}\,(x_i),\ tp(\gamma) = \min_i tp(x_i),\ ht(\gamma) = \inf_i ht(x_i).$$

La partie L_V de L est définie par les conditions $x_i \in E_V$ pour tout $i \in I$, et la topologie de L est définie comme celle de E au moyen de la fonction ord.

(4.4) Théorème. *Soient, pour $p \in S$ et $i \in I$, des éléments $u_{p,i}$ de L tels que $ht(u_{p,i}) \geqslant (1/p)+$. Posons $\varepsilon_{p,i} = F_p\gamma_i - u_{p,i}$. Alors il existe un projecteur $\pi_V : L \to L_V$ ($\pi_V \circ \pi_V = \pi_V$) et des fonctions $f_{p,i} : L \to E$ vérifiant les propriétés suivantes*:

(4.4.1) *pour tout $\gamma \in L$, $\gamma = \pi_V(\gamma) + \sum_{p \in S,\, i \in I} f_{p,i}(\gamma)\varepsilon_{p,i}$ (et $\mathrm{ord}\,(f_{p,i}(\gamma)) \to \infty$ quand I est infini)*;

(4.4.2) $tp(\gamma) = \min\,(tp(\pi_V(\gamma)), (tp(f_{p,i}(\gamma)F_p))_{(p,i) \in S \times I})$;

(4.4.3) $ht(\gamma) = \inf\,(ht(\pi_V(\gamma)), (ht(f_{p,i}(\gamma)F_p))_{(p,i) \in S \times I})$.

De plus, les fonctions $f_{p,i}$ et le projecteur π_V sont fonctoriels en K, en un sens facile à préciser.

Désignons par N le sous-module fermé de L engendré par les $\varepsilon_{p,i}$ ($p \in S$, $i \in I$) et par C le E-module uniforme quotient L/N. D'après (4.4.1), *les images des γ_i dans C sont une famille de V-générateurs.*

(4.5) Théorème. *Les trois propriétés suivantes sont équivalentes et sont toujours vérifiées si* Card $(S)=1$:

(4.5.1) *les images des* γ_i $(i \in I)$ *constituent une* V*-base de* C;

(4.5.2) *pour tout* $\gamma \in N$, $\gamma \neq 0$, *on a* $tp(\gamma) < (\mathrm{ord}\,(\gamma), 1)$;

(4.5.3) *en posant* $\delta_{p,q,i} = F_q \varepsilon_{p,i} - F_p \varepsilon_{q,i}$, *on a* $\pi_V(\delta_{p,q,i}) = 0$ *pour tous* $p, q \in S$ *et tout* $i \in I$.

(4.6) Exemple. Posons $I' = I \cup \{\omega\}$ où $\omega \notin I$ et soient des applications $\sigma_p : I' \to I'$ telles que $\sigma_p(\omega) = \omega$ et $\sigma_p \circ \sigma_q = \sigma_q \circ \sigma_p$ pour tous $p, q \in S$. Convenons que $\gamma_\omega = 0$. Alors les éléments $u_{p,i} = \gamma_{\sigma_p(i)}$ vérifient la condition (4.5.3), et les modules réduits ainsi obtenus correspondent à des groupes formels qui généralisent les covecteurs et bivecteurs de Witt introduits par I. Barsotti [4]). Cet exemple sera repris plus loin (III.4).

II. Equivalence de catégories; équations de structure

1. *Variétés et groupes formels.* Nous reprenons la définition des variétés formelles comme foncteurs en ensembles donnée par Cartier, à ceci près que nous introduisons des variétés de dimension (éventuellement) *infinie* et que nous utilisons sur un anneau K, la catégorie "$\mathbf{nil}_K$" des K-algèbres (non unitaires) dont tous les éléments sont *nilpotents*. Nous dirons ici "variété" au lieu de "variété *formelle*" et "groupe formel" au lieu de "groupe formel *commutatif*". Nous notons P l'ensemble de tous les nombres premiers et $\mathbf{P}$ celui des entiers $\geqslant 1$; nous écrivons Cart(K) au lieu de Cart$_P(K)$.

La "droite formelle" D (ou D_K) devient ainsi le foncteur identique sur $\mathbf{nil}_K$. Pour tout ensemble I, nous avons le *modèle* $D^{(I)}$ dont les points à coordonnées dans $A \in \mathbf{nil}_K$ sont les familles $\mathbf{x} = (x_i)_{i \in I}$ d'éléments de A *presque tous nuls.* Une variété de dimension Card (I) est alors isomorphe à $D^{(I)}$ les morphismes étant définis comme chez Cartier (*morphismes de foncteurs en ensembles pointés*). Nous désignons par $\mathscr{M}(V, W)$ l'ensemble des morphismes d'une variété V dans une variété W; nous notons $\mathscr{C}(V)$ l'ensemble $\mathscr{M}(D, V)$ des *courbes* dans V et $\mathscr{F}(V)$ l'ensemble $\mathscr{M}(V, D)$ des fonctions sur V (à terme constant nul).

(1.1) Lemme. *Soient* $f, f' \in \mathscr{M}(V, W)$ *tels que pour tout* $\varphi \in \mathscr{C}(V)$ $f \circ \varphi = f' \circ \varphi$. *Alors* $f = f'$.

(1.2) Chaque ensemble de morphismes possède une filtration naturelle notée "ord", à valeurs dans $\mathbf{P}$, vérifiant "ord $(f \circ g) \geqslant$ ord (f) ord (g)" quand f, g sont deux morphismes composables. Pour tout $r \in \mathbf{P}$, la relation "ord $(f - f') > r$" où $f, f' \in \mathscr{M}(V, D^{(I)})$ ne dépend que de la structure de variété de $D^{(I)}$ (bien que sa définition fasse intervenir la structure additive),

---

[4]) I. Barsotti, Metodi analitici per varietà abeliane in caratteristica positiva. Cap. 1,2 (Ann. Sc. Norm. Sup. Pisa Sc. Fis. Mat. ser. III, 18 (1964) p. 1–25).

ce qui nous permet d'écrire cette relation plus généralement sous la forme "$f \equiv f'$ (mod. deg. $r+1$)" pour $f, f' \in \mathscr{M}(V, W)$. La classe d'équivalence de f (mod. deg. $r+1$) est appelée r-jet de f. En particulier le 1-jet de $\gamma \in \mathscr{C}(V)$, noté $\mathscr{T}\gamma$, est un vecteur tangent à V ("vitesse" de γ); l'ensemble des $\mathscr{T}\gamma$ est l'*espace tangent à* V, noté $\mathscr{T}V$, qui possède une structure naturelle de K-*module libre*. Nous définissons une *famille basique* dans $\mathscr{C}(V)$ comme une famille $(\gamma_i)_{i \in I}$ telle que $(\mathscr{T}\gamma_i)_{i \in I}$ soit une base de $\mathscr{T}V$ sur K.

(1.3) Dans un groupe formel G, une famille basique de courbes $(\gamma_i)_{i \in I}$ définit un système de coordonnées, dites "*curvilignes*", grâce à l'isomorphisme $D^{(I)} \to G$ donné par $\mathbf{x} \mapsto \sum_{i \in I} \gamma_i(x_i)$, où $\mathbf{x} \in A^{(I)}$, $A \in \mathbf{nil}_K$.

(1.4) Un homomorphisme d'anneaux, $f: K \to K'$, définit un foncteur (changement d'anneau de base) qui transforme une variété V sur K en une variété sur K', notée ${}_fV$. L'application de $\mathscr{M}_K(V, W)$ dans $\mathscr{M}_{K'}({}_fV, {}_fW)$ est injective (resp. surjective) si f est injectif (resp. surjectif): en effet, pour les modèles, cette application s'obtient en transformant par f les coefficients des séries formelles qui définissent les morphismes.

2. *Le théorème* 1 *de Cartier et ses premières conséquences* [2.2]). Les opérateurs V_n ($n \in \mathbf{P}$) et $[c]$ ($c \in K$) sont définis "au départ" sur les ensembles de courbes $\mathscr{C}(V)$ où V est une variété quelconque sur K. Par contre, les opérateurs F_n ($n \in \mathbf{P}$) sont propres aux *groupes* formels.

Soit $\hat{W}_K{}^+$ le groupe formel additif des vecteurs de Witt sur K et γ_w sa courbe canonique, si bien que tout élément $\mathbf{x} \in \hat{W}_K{}^+(A)$ s'écrit

$$\mathbf{x} = \textstyle\sum_{n \in \mathbf{P}} (F_n \cdot \gamma_w)(x_n), \text{ où } x_n \in A,\ A \in \mathbf{nil}_K. \tag{2.1}$$

Soient G un groupe formel sur K et $\gamma \in \mathscr{C}(G)$. *Le théorème* 1 *de Cartier affirme l'existence et l'unicité de* $u \in \mathrm{Hom}\,(\hat{W}_K{}^+, G)$ *tel que* $u \circ \gamma_w = \gamma$. D'après (2.1), tout revient à vérifier l'énoncé suivant. Soient $\mathbf{x}, \mathbf{y}, \mathbf{z} \in A^{(\mathbf{P})}$ vérifiant la relation

$$\textstyle\prod_{n \in \mathbf{P}} (1 - x_n T^n)(1 - y_n T^n) = \prod_{n \in \mathbf{P}} (1 - z_n T^n), \tag{2.2}$$

où T est une indéterminée. Alors

$$\textstyle\sum_{n \in \mathbf{P}} ((F_n \cdot \gamma)(x_n) + (F_n \cdot \gamma)(y_n)) = \sum_{n \in \mathbf{P}} (F_n \cdot \gamma)(z_n) \tag{2.3}$$

dans le groupe $G(A)$. On prouve successivement cette assertion dans les cas suivants: 1°) G est un groupe additif (additivité des "composantes fantômes" des vecteurs de Witt); 2°) K est une $\mathbf{Q}$-algèbre (réduction au 1°), puisque G est isomorphe à un groupe formel additif); 3°) K est sans torsion additive (réduction au 2°) par plongement de K dans $\mathbf{Q} \otimes K$); 4°) le cas général se réduit au 3°) grâce au "théorème des fantômes" suivant.

(2.4) *Soit G un groupe formel défini sur un anneau K. Alors il existe un anneau K_0 sans torsion additive, un épimorphisme $f: K_0 \to K$ et un groupe formel G_0 sur K_0 tel que G soit isomorphe à ${}_fG_0$.*

La considération des lois de groupes et bourgeons *curvilignes* facilite considérablement la réduction de la preuve de ce théorème au cas de la dimension 1 [5]).

(2.5) On vérifie que chaque courbe $\gamma \in \mathscr{C}(\hat{W}_K{}^+)$ s'écrit univoquement sous la forme $x \cdot \gamma_w$, où $x \in \mathrm{Cart}\,(K)$. On en déduit que, *pour tout groupe formel* G, $\mathscr{C}(G)$ *est un* Cart (K)*-module réduit* (1.3), $\mathscr{C}(\hat{W}_K{}^+)$ *étant un* Cart (K)*-module libre de générateur canonique* γ_w.

(2.6) A chaque $\varphi \in \mathscr{C}(D) = \mathscr{F}(D)$ correspond un élément $\mathrm{comp}\,(\varphi) \in \mathrm{Cart}\,(K)$ défini par la relation $\gamma_w \circ \varphi = \mathrm{comp}\,(\varphi) \cdot \gamma_w$ *et cette relation reste valable quand on y remplace* γ_w *par n'importe quelle courbe* γ *dans un groupe formel* G. Si $\varphi(t) = ct^n$, alors $\mathrm{comp}\,(\varphi) = V_n[c]$; pour tous $\varphi, \varphi' \in \mathscr{C}(D)$ on a $\mathrm{comp}\,(\varphi \circ \varphi') = \mathrm{comp}\,(\varphi')\,\mathrm{comp}\,(\varphi)$ et

$$\text{(2.7)} \qquad \mathrm{ord}\,(\mathrm{comp}\,(\varphi + \varphi') - \mathrm{comp}\,(\varphi) - \mathrm{comp}\,(\varphi')) \geqslant \mathrm{ord}\,(\varphi) + \mathrm{ord}\,(\varphi').$$

(2.8) Chaque endomorphisme u de $\hat{W}_K{}^+$ est défini par la donnée de $u \circ \gamma_w = x_u \cdot \gamma_w$ où $x_u \in \mathrm{Cart}\,(K)$, ce qui permet d'identifier l'anneau $\mathrm{End}\,(\hat{W}_K{}^+)$ à Cart (K) opérant *à droite* sur les groupes $\hat{W}_K{}^+(A)$, $A \in \mathbf{nil}_K$, selon la formule

$$\left(\textstyle\sum_{n \in \mathbf{P}} (F_n \cdot \gamma_w)(t_n)\right) \cdot x = \textstyle\sum_{n \in \mathbf{P}} (F_n x \cdot \gamma_w)(t_n),$$

où $x \in \mathrm{Cart}\,(K)$, $t_n \in A$. Si on considère $\hat{W}_K{}^+(A)$ comme plongé dans le groupe $W^+(A)$, sur lequel Cart (K) opère *à gauche*, on a les formules (fâcheuses, mais qu'y faire?)

$$V_n \cdot (\gamma_w(t)) = (F_n \cdot \gamma_w)(t) \quad \text{et} \quad F_n \cdot (\gamma_w(t)) = (V_n \cdot \gamma_w)(t),$$

où $t \in A$, $n \in \mathbf{P}$, tandis que, pour tout $c \in K$, $[c] \cdot (\gamma_w(t)) = ([c] \cdot \gamma_w)(t)$.

3. *Le théorème* 2 *de Cartier* [2.2]). Il s'agit de prouver que le foncteur $G \to \mathscr{C}(G)$, qui transforme un groupe formel sur K en un Cart (K)-module réduit est *pleinement fidèle*. Autrement dit, quels que soient les groupes formels G, G' sur K, toute application Cart (K)*-linéaire continue*, $f : \mathscr{C}(G) \to \mathscr{C}(G')$, provient d'un homomorphisme unique $u \in \mathrm{Hom}\,(G, G')$ par la relation $f(\gamma) = u \circ \gamma$, $\gamma \in \mathscr{C}(G)$. Pour démontrer cela, considérons un groupe formel comme un groupe dans la catégorie des variétés sur K. Il s'agit donc de construire, pour toute variété V, l'homomorphisme de groupes $\mathscr{M}(V, G) \to \mathscr{M}(V, G')$, qui sera obtenu par composition avec l'homomorphisme u cherché: à $g \in \mathscr{M}(V, G)$ correspondra $g' = u \circ g \in \mathscr{M}(V, G')$. Pour tout $\varphi \in \mathscr{C}(V)$ on doit donc avoir

$$\text{(3.1)} \qquad g' \circ \varphi = f(g \circ \varphi).$$

D'après le lemme (1.1), il suffit de montrer l'*existence* de g' vérifiant (3.1). On vérifie que les $g \in \mathscr{M}(V, G)$ pour lesquels g' existe forment un sous-

[5]) Cf. M. Lazard, Sur les groupes de Lie formels à un paramètre. Bull. Soc. Math. Fr. 83 (1955), p. 251–274. Nous exposerons ultérieurement ce qui remplace la loi de groupe universelle dans le cas d'une dimension infinie.

groupe fermé de $\mathscr{M}(V, G)$ contenant tous les morphismes décomposables $g=g_1 \circ g_2$, où $g_1 \in \mathscr{C}(G)$, $g_2 \in \mathscr{F}(V)$, pour lesquels $g'=f(g_1) \circ g_2$. Or, si $(\gamma_i)_{i\in I}$ est une famille basique dans $\mathscr{C}(G)$, tout morphisme $g \in \mathscr{M}(V, G)$ s'écrit univoquement $g= \sum_{i\in I} \gamma_i \circ h_i$, où $h_i \in \mathscr{F}(V)$.

4. *Le théorème* 3 *de Cartier* [2.2]). Il s'agit de prouver que tout Cart (K)-module réduit C est isomorphe au module $\mathscr{C}(G)$ des courbes d'un groupe formel G sur K. Pour cela nous allons construire les groupes $\mathscr{M}(V, G)$ où V est une variété sur K. Considérons le groupe *filtré complet* Γ_V défini par générateurs et relations (i.e. comme solution d'un problème d'application universelle dans la catégorie des groupes filtrés complets). Les générateurs de Γ_V sont notés $\gamma \square \varphi$ où $\gamma \in C$ et $\varphi \in \mathscr{F}(V)$; ils vérifient les relations ord $(\gamma \square \varphi) \geqslant$ ord (φ) et $\sum_{j\in J} (\gamma_j \square \varphi_j)=0$ quand $\sum_{j\in J}$ comp $(\varphi_j \circ \psi)\cdot\gamma_j=0$ pour tout $\psi \in \mathscr{C}(V)$. A chaque morphisme $f\colon V \to W$ correspond un homomorphisme de groupes $\Gamma_W \to \Gamma_V$ défini sur les générateurs $\gamma \square \varphi$ (où $\gamma \in C, \varphi \in \mathscr{F}(W)$) par $\gamma \square \varphi \mapsto \gamma \square (\varphi \circ f)$. Pour montrer que le foncteur Γ est représentable, nous choisissons une V-base $(\gamma_i)_{i\in I}$ de C et nous prouvons d'abord, en appliquant (2.7), que tout élément $\gamma \in C$ s'écrit univoquement $\sum_{i\in I}$ comp $(\varphi_i)\cdot \gamma_i$ avec des $\varphi_i \in \mathscr{F}(D)$, tels que ord $(\varphi_i) \to \infty$ quand I est infini. Ensuite nous montrons que tout élément g de Γ_V s'écrit univoquement $\sum_{i\in I} \gamma_i \square \varphi_i$, avec des $\varphi_i \in \mathscr{F}(V)$ (tendant vers 0 quand I est infini) et ord $(g)=$ $\min_i$ ord (φ_i). Cela entraîne l'existence du groupe formel G cherché, tel que C s'identifie à Γ_D et à $\mathscr{C}(G)$.

Les trois théorèmes de Cartier se résument en disant que *la catégorie des groupes formels sur K est équivalente à celle des* Cart (K)-*modules réduits.* Nous indiquerons ultérieurement d'autres démonstrations des théorèmes 2 et 3 faisant intervenir des produits tensoriels.

5. *Cas où certains nombres premiers sont inversibles dans l'anneau de base.* Soient S une partie non vide de P et S' son complémentaire. Quand tous les $p \in S$ sont inversibles dans K, la catégorie des Cart (K)-modules réduits est équivalente à celle des $\mathrm{Cart}_{S'}(K)$-modules réduits (I.3.3). Le $\mathrm{Cart}_{S'}(K)$-module correspondant ainsi à un groupe formel G est l'ensemble des courbes $\gamma \in \mathscr{C}(G)$ qui sont annulées par tous les F_q où $q \in S$; ces courbes sont dites S'-typiques, ou p-typiques quand $S'=\{p\}$.

6. *Equations de structure.* Soient G un groupe formel et $(\gamma_i)_{i\in I}$ une famille basique dans $\mathscr{C}(G)$. Considérons une famille de relations dans $\mathscr{C}(G)$, de la forme

$$F_p\cdot\gamma_i= \sum_{j\in I} x_{p,i,j}\cdot\gamma_j, \tag{6.1}$$

où $p \in P$, $i \in I$, $x_{p,i,j} \in$ Cart (K), $ht(x_{p,i,j}) \geqslant (1/p)+$ (et ord $(x_{p,i,j}) \to \infty$ avec j pour tous p, i quand I est infini).

D'après l'équivalence de catégories et le théorème (I.4.4), les relations (6.1) définissent complètement la structure du groupe formel G, ou, plus précisément, déterminent la loi de groupe sur $D^{(I)}$ correspondant aux coordonnées curvilignes de G associées aux γ_i. Nous disons que (6.1) est un système d'*équations de structure* de G. En particulier, on peut prendre les $x_{p,i,j}$ de la forme

$$x_{p,i,j} = \sum_{n \in \mathbf{P}} V_n[c_{n,p,i,j}], \tag{6.2}$$

avec des éléments $c_{n,p,i,j} \in K$, univoquement déterminés, que nous appelons "*constantes de structure*" associées à la famille (γ_i).

Réciproquement, un système d'équations de la forme (6.1) définit un groupe formel *pourvu que les conditions équivalentes du théorème* (I.4.5) *soient satisfaites*. Nous reviendrons ultérieurement sur les relations que vérifient les constantes de structure $c_{n,p,i,j}$. Signalons seulement un cas particulier important où les équations (6.1) définissent un groupe formel: pour un certain nombre premier p, pour tout $q \in P$, $q \neq p$, et tous $i, j \in I$, on a

$$x_{q,i,j} = 0 \quad \text{et} \quad F_q x_{p,i,j} \in \operatorname{Cart}(K)\, F_q \quad \text{(idéal à gauche)}. \tag{6.3}$$

(To be continued)